

# Threat Reports

Login 

Menu ()

()

23rd November 2017

| Tags: daily cyber digest

(<https://www.silobreaker.com/tag/daily-cyber-digest/>)

Silobreaker  
Daily Cyber  
Digest – 23  
November  
2017

# silobreaker

## Daily Cyber Digest

23/11/17

Malware | Attack Types | Leaks & Breaches | Campaigns | Vulnerabilities

(<https://www.silobreaker.com/wp-content/uploads/2017/11/231117.png>)

Login 

Menu 

### Malware

Trend Micro reports on macro-based  
qkG Filecoder ransomware

> QkG Filecoder

([https://my.silobreaker.com/view360.aspx?](https://my.silobreaker.com/view360.aspx?item=11_1434342000#?)  
[item=11\\_1434342000#?](https://my.silobreaker.com/view360.aspx?item=11_1434342000#?)

[q=Malware:%22qkG%20Ransomware%22&rd=true](https://my.silobreaker.com/view360.aspx?q=Malware:%22qkG%20Ransomware%22&rd=true))

is a file-encrypting ransomware entirely  
written in VBA macros.

> The macros lower Word's security  
settings and infect the normal.dot template,  
loading malicious code into every Word  
instance. When a user closes a document,  
the file's contents will be encrypted.

> The threat actor, allegedly located in  
Vietnam and going by the name TNA-MHT-  
TT2

([https://my.silobreaker.com/view360.aspx?](https://my.silobreaker.com/view360.aspx?item=11_1433490809#?)  
[item=11\\_1433490809#?](https://my.silobreaker.com/view360.aspx?item=11_1433490809#?)

[q=ThreatActor:%22TNA-MHT-  
TT2%22&rd=true](https://my.silobreaker.com/view360.aspx?q=ThreatActor:%22TNA-MHT-TT2%22&rd=true)), is demanding a ransom  
of \$300 in Bitcoin.

– Source

(<http://blog.trendmicro.com/trendlabs-security-intelligence/qkg-filecoder-self-replicating-document-encrypting-ransomware/>) –

## Ongoing Campaigns

McAfee reports on the increase in cybercriminal use of malware miners   ()

> The increase in illegal mining is directly correlated to the increase in value of cryptocurrencies, particularly Bitcoin, which has been rising in value for years.

> Cybercriminals have been innovating malware such as Dridex  
([https://my.silobreaker.com/view360.aspx?item=11\\_773406215#?](https://my.silobreaker.com/view360.aspx?item=11_773406215#?q=Malware%3a%22Dridex+Malware%22&rd=true)

[q=Malware%3a%22Dridex+Malware%22&rd=true](https://my.silobreaker.com/view360.aspx?item=11_773406215#?q=Malware%3a%22Dridex+Malware%22&rd=true))  
and Trickbot

([https://my.silobreaker.com/view360.aspx?item=11\\_1074676862#?](https://my.silobreaker.com/view360.aspx?item=11_1074676862#?q=Malware:%22Trickbot%20Malware%22&rd=true)  
[q=Malware:%22Trickbot%20Malware%22&rd=true](https://my.silobreaker.com/view360.aspx?item=11_1074676862#?q=Malware:%22Trickbot%20Malware%22&rd=true))

to include crypto-mining functions, which bypass the formal agreement stage and use a victim's computing power to mine for coins or locate and steal the user's cryptocurrency.

> McAfee reports that in September cybercriminals stole \$63,000 worth of cryptocurrency in three months by taking

advantage of a flaw in Microsoft Windows

Internet information Services.

– Source

([https://securingtomorrow.mcafee.com/mcafee-labs/malware-mines-steals-](https://securingtomorrow.mcafee.com/mcafee-labs/malware-mines-steals-cryptocurrencies-from-victims/)

[cryptocurrencies-from-victims/](https://securingtomorrow.mcafee.com/mcafee-labs/malware-mines-steals-cryptocurrencies-from-victims/)) –

The Trickbot banking trojan gang is now using hybrid account checking attacks

> The group, reportedly the successor of the Dyre Wolf cyber gang

([https://my.silobreaker.com/View360.aspx?](https://my.silobreaker.com/View360.aspx?Item=11_844493667&q=ThreatActor%3A%22Dyre%20Wolf%20Cyber%20Gang%22)

[Item=11\\_844493667&q=ThreatActor%3A%22Dyre%20Wolf%20Cyber%](https://my.silobreaker.com/View360.aspx?Item=11_844493667&q=ThreatActor%3A%22Dyre%20Wolf%20Cyber%20Gang%22)

are using new attack methods. They are

also expanding from targeting the financial

sector to attack Russian and US-based

companies in gaming, tech, cryptocurrency

and other industries.

> The hackers are distributing spam emails delivering Trickbot

([https://my.silobreaker.com/View360.aspx?](https://my.silobreaker.com/View360.aspx?Item=11_1074676862&q=Malware%3A%22Trickbot%20Malware%22)

[Item=11\\_1074676862&q=Malware%3A%22Trickbot%20Malware%22](https://my.silobreaker.com/View360.aspx?Item=11_1074676862&q=Malware%3A%22Trickbot%20Malware%22)).

Upon infection, the victim's machine will

download the backconnect SOCKS5 proxy

module, allowing the hackers to enlist the

machine's IP as its proxy.

> They will then use victim IPs as proxies to leverage username and password

combinations for account checking activity.

Since the gang's IP address is the same as

its victims', the target companies' anti-fraud

systems will not be able to detect the

attack.

– Source (<https://www.flashpoint-intel.com/blog/trickbot-account-checking-hybrid-attack-model/>) –

Possible Ukraine cyber gang targeting Canadian banking customers with phishing attacks

> IBM Xforce research said the attacks start with a spear phishing email that tricks stakeholders with account access to reveal their firm's banking credentials, passwords and two-factor authentication codes. The attackers then take over the account and transfer funds to mule accounts in their control.

> The criminals crafted customised PDF files that seemed to come from workers at the targeted businesses' banks, and urged victims to open the files to avoid canceled and delayed payments and transactions.

– Source

(<https://securityintelligence.com/canadian-business-banking-customers-hit-with-targeted-phishing-account-takeover-attacks/>) –

€100,000 of Bitcoin allegedly stolen by hackers using a fake WiFi network

> Austrian police report that the victim logged into a restaurant's WiFi network on an "unknown, non-traceable account" to check the value of their Bitcoin.

Login 

Menu () ()

> It is unclear if the Bitcoins had already been stolen prior to logging onto the network.

– Source (<http://www.ibtimes.co.uk/fake-wifi-network-used-by-hackers-steal-more-100000-worth-bitcoin-1648424>) –

## Leaks & Breaches

Login 

Menu ()

Uber denies unauthorised customer transactions in Singapore are linked to its 2016 global data breach

> The cab-hailing firm said the data breach did not contain financial information and is thus unrelated. Some customers in Singapore have noted account and credit card charges for Uber rides they did not take in foreign countries.

– Source 1

(<http://www.zdnet.com/article/uber-says-unauthorised-transactions-in-singapore-not-linked-to-global-breach/>) – Source 2

(<http://www.channelnewsasia.com/news/singapore/uber-users-in-singapore-charged-for-phantom-rides-overseas-9423624>) –

## Vulnerabilities

Samba release patches for two vulnerabilities affecting SAMBA 4.0 and versions 3.6.0 onwards

> CVE-2017-14746

([https://my.silobreaker.com/view360.aspx?item=11\\_1432506931#?](https://my.silobreaker.com/view360.aspx?item=11_1432506931#?)

q=Vulnerability:%22CVE-2017-

14746%22&rd=true) is a use-after-free error

affecting all versions of SAMBA since 4.0.

The bug allows an attacker to gain control

over 'the contents of heap memory via a deallocated heap pointer', and possibly compromise the SMB server, through a malicious SMB1 request.

> CVE-2017-15275

([https://my.silobreaker.com/view360.aspx?item=11\\_1432506932#?](https://my.silobreaker.com/view360.aspx?item=11_1432506932#?)

q=Vulnerability:%22CVE-2017-

15275%22&rd=true) affects all versions of SAMBA from 3.6.0 onwards, leaving them vulnerable to a 'heap memory information leak, where the server allocated heap memory may be returned to the client without being cleared.' These leaks may contain hashed passwords, or other credentials.

– Source 1

(<https://www.samba.org/samba/security/CVE-2017-14746.html>) – Source 2

(<https://www.samba.org/samba/security/CVE-2017-15275.html>) –

Login 

Menu () ()

CVE-2017-11826 exploited in politically themed malware campaign

> Fortinet reports that a malicious RTF file is utilised to deliver the malicious payload by abusing CVE-2017-11826

([https://my.silobreaker.com/view360.aspx?item=11\\_1394070354#?](https://my.silobreaker.com/view360.aspx?item=11_1394070354#?)

q=Vulnerability:%22CVE-2017-

11826%22&rd=true), an object-handling vulnerability in Microsoft Office already

patched in November.

> The content of the RTF file initially displays text about Aqua Mul Mujahidin, a jihadist group. After the exploit triggers, another document containing text from an article called Saudi Arabia's 'Game of Thrones' appears.

> The campaign is reportedly a targeted attack on specific institutions, rather than a full scale cyber crime campaign.

– Source

(<https://blog.fortinet.com/2017/11/22/cve-2017-11826-exploited-in-the-wild-with-politically-themed-rtf-document>) –

Arbitrary code execution vulnerability in 54 HP Inc printer models patched

> FoxGlove Security picked up on the vulnerability first in the firm's PageWide Enterprise Color MFP 586 and Color LaserJet Enterprise M553 printer models.

FoxGlove informed HP in August and both

Login 

Menu () ()



coordinated the bug's disclosure for this week.

> The bug allowed researchers to execute code on the printers by reverse engineering .BDL extension files used in HP Solutions and firmware updates. CVE-2017-2750 ([https://my.silobreaker.com/view360.aspx?item=11\\_1433483786#?q=Vulnerability:%22CVE-2017-2750%22&rd=true](https://my.silobreaker.com/view360.aspx?item=11_1433483786#?q=Vulnerability:%22CVE-2017-2750%22&rd=true)) was linked to

'insufficient solution DLL signature validation', making it possible for a

potential attacker to run malware on an affected printer.

– Source 1 (<https://support.hp.com/nz-en/document/c05839270>) – Source 2 (<https://foxglovesecurity.com/2017/11/20/a-sheep-in-wolfs-clothing-finding-rce-in-hps-printer-fleet/>) –

The Silobreaker Team

*Disclaimer: Although Silobreaker has relied on what it regards as reliable sources while compiling the content herein, Silobreaker cannot guarantee the accuracy, completeness, integrity or quality of such content and no responsibility is accepted by Silobreaker in respect of such content. Readers must determine for themselves what reliance they should place on the compiled content herein.*

# More News

(<https://www.silobreaker.com/silobreaker-daily-cyber-digest-09-march-2018/>)

9 March 2018

## Silobreaker Daily Cyber Digest – 09 March 2018

Login



Menu

()

()

Malware Microsoft Windows Defender blocks 80,000 instances of new variants of the Dofail downloader Microsoft have stated that the Dofail downloader, also known...

(<https://www.silobreaker.com/silobreaker-daily-cyber-digest-09-march-2018/>)

(<https://www.silobreaker.com/silobreaker-daily-cyber-digest-08-march-2018/>)

8 March 2018

## Silobreaker Daily Cyber Digest – 08 March 2018

Malware FlawedAmmy RAT discovered by ProofPoint ProofPoint researchers state that the trojan has been used since the start of 2016 in both targeted email...

Login 

Menu ()

[\(https://www.silobreaker.com/silobreaker-daily-cyber-digest-08-march-2018/\)](https://www.silobreaker.com/silobreaker-daily-cyber-digest-08-march-2018/)

()

[\(https://www.silobreaker.com/silobreaker-daily-cyber-digest-07-march-2018/\)](https://www.silobreaker.com/silobreaker-daily-cyber-digest-07-march-2018/)

7 March 2018

## Silobreaker Daily Cyber Digest – 07 March 2018

Malware Gozi ISFP banking trojan using Dark Cloud botnet for distribution  
Talos observed Gozi ISFB using Dark Cloud for distribution, Nymaim command  
and...

[\(https://www.silobreaker.com/silobreaker-daily-cyber-digest-07-march-2018/\)](https://www.silobreaker.com/silobreaker-daily-cyber-digest-07-march-2018/)

[View all News \(/news/\)](/news/)

## Request a demo

[Login](#) [Menu](#) ()

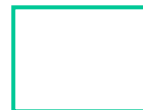
()

[Get in touch](/contact-us#demo-form)[\(/contact-us#demo-form\)](/contact-us#demo-form)

## Get in touch with us

[sales@silobreaker.com](mailto:sales@silobreaker.com) (<mailto:sales@silobreaker.com>) | [support@silobreaker.com](mailto:support@silobreaker.com)  
(<mailto:support@silobreaker.com>)

## Sign up for product and company updates



[Cyber Security \(https://www.silobreaker.com/how-its-used/cyber-security/\)](https://www.silobreaker.com/how-its-used/cyber-security/)

[Home \(https://www.silobreaker.com/\)](https://www.silobreaker.com/)

[Who We Are \(https://www.silobreaker.com/who-we-are/\)](https://www.silobreaker.com/who-we-are/)

[How It Works \(https://www.silobreaker.com/how-it-works/\)](https://www.silobreaker.com/how-it-works/)

[Features \(https://www.silobreaker.com/features/\)](https://www.silobreaker.com/features/)

[Products \(https://www.silobreaker.com/products/\)](https://www.silobreaker.com/products/)

[News & Views \(https://www.silobreaker.com/news-and-views/\)](https://www.silobreaker.com/news-and-views/)

[Threat Reports \(https://www.silobreaker.com/threat-reports/\)](https://www.silobreaker.com/threat-reports/)

[Contact \(https://www.silobreaker.com/contact-us/\)](https://www.silobreaker.com/contact-us/)

[Legal \(/legal/\)](/legal/) ©2018 Silobreaker

Login 

Menu ()

()